UNITED STATES DISTRICT COURT
For the Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DANIEL J. BERNSTEIN,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF COMMERCE, et al.,

Defendants.

_____/

No. C 95-0582 MHP

MEMORANDUM AND ORDER
Motions for Summary Judgment

Plaintiff Daniel Bernstein filed a second supplemental complaint in this action alleging that export regulations administered by defendant United States Department of Commerce are in violation of the First, Fourth and Fifth Amendments, both facially and as applied to plaintiff's cryptographic research. Among other claims, Bernstein alleges that the revised regulations are impermissibly content-based, constitute a prior restraint, and are vague and overbroad. Defendants now bring a motion to dismiss, or in the alternative for summary judgment,[1] and plaintiff brings a cross-motion for summary judgment. Having considered the arguments presented, and for the reasons set forth below, the court rules as follows.

BACKGROUND[2]

Bernstein is an associate professor in the Department of Mathematics, Statistics, and Computer Science at the University of Illinois at Chicago. Bernstein Dec. Supp. Pl.'s Mot. Summ. J. ¶ 7. Bernstein's research interests include cryptography, a field of applied mathematics that uses computer programs to encrypt electronic communications. Encryption converts a set of data into code, which can ensure data integrity, authenticate users, link messages to their senders, and maintain confidentiality.

Initially, the Arms Export Control Act, 22 U.S.C. § 2278, and the International Traffic in Arms Regulations ("ITAR"), 22 C.F.R. §§ 120–30, limited the export of encryption items. All items placed on the United States Munitions List ("USML") required a license for export. An exporter could submit an item to the United States Department of State under a "commodity jurisdiction procedure" to determine whether the item was controlled by ITAR. On June 30, 1992, Bernstein submitted source code for an encryption algorithm he called "Snuffle," together with accompanying papers explaining the program, to the Department of State. The Department of State determined that "Snuffle" was a defense article subject to the USML, and thus required a license for export.

In 1995, Bernstein brought this action against the Department of State and individually named defendants seeking declaratory and injunctive relief from enforcement of the Arms Export Control Act and ITAR on the grounds that they were unconstitutional on their face and as applied to him. This court denied defendants' motion to dismiss and held that for purposes of First Amendment analysis, source code is speech. Bernstein v. United States Dept. of State, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996). Subsequently, on cross-motions for summary judgment, this court held that the ITAR licensing scheme with regard to encryption items was an unconstitutional prior restraint. Bernstein v. United States Dept. of State, 974 F. Supp. 1288, 1290 (N.D. Cal. 1997). This court also held that two license exceptions were void for vagueness. Id. at 1294.

In November 1996, before this court issued its order on the cross-motions for summary judgment, the President of the United States transferred jurisdiction over the export of nonmilitary encryption products to the United States Department of Commerce. Exec. Order No. 13,206, 61 Fed. Reg. 58,767 (Nov. 15, 1996). The transferred encryption items were thereafter subject to the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730 et seq.. On December 30, 1996, the Bureau of Export Administration, now the Bureau of Industry and Security ("BIS"), issued an interim rule on export of encryption items. 61 Fed. Reg. 68,572 (Dec. 30, 1996). Bernstein supplemented his complaint to add the new rule and the Department of Commerce as a defendant. On cross-motions for summary judgment, this court held that the regulation of encryption items, which was identical in effect to the ITAR requirements, constituted an

unconstitutional prior restraint on speech. Bernstein v. United States Dept. of State, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997). The court then granted declaratory and injunctive relief. Id. at 1310.

On appeal to the Ninth Circuit, the panel upheld this court's 1997 decision. Specifically, the panel held that "encryption software, in its source code form and as employed by those in the field of cryptography, must be viewed as expressive," and that the encryption regulations were an unconstitutional prior restraint on speech. Bernstein v. United States Dept. of Justice, 176 F.3d 1132, 1141, 1145 (9th Cir. 1999). The Ninth Circuit then voted to rehear the action *en banc* and withdrew the panel decision. Bernstein v. United States Dept. of Justice, 192 F.3d 1308, 1309 (9th Cir. 1999). Before the action was heard *en banc*, the Department of Commerce issued regulations amending the EAR's encryption provisions. 65 Fed. Reg. 2492 (Jan. 14, 2000). The action was then remanded to this court for further proceedings.

LEGAL STANDARD

Summary judgment is proper when the pleadings, discovery and affidavits show that there is "no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). Material facts are those which may affect the outcome of the case. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986). A dispute as to a material fact is genuine if there is sufficient evidence for a reasonable jury to return a verdict for the nonmoving party. Id. The moving party for summary judgment bears the burden of identifying those portions of the pleadings, discovery and affidavits that demonstrate the absence of a genuine issue of material fact. Celotex Corp. v. Cattrett, 477 U.S. 317, 323 (1986). On an issue for which the opposing party will have the burden of proof at trial, the moving party need only point out "that there is an absence of evidence to support the nonmoving party's case." Id.

Once the moving party meets its initial burden, the nonmoving party must go beyond the pleadings and, by its own affidavits or discovery, "set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e). Mere allegations or denials do not defeat a moving party's allegations. Id.; see also Gasaway v. Northwestern Mut. Life Ins. Co., 26 F.3d 957, 960 (9th Cir. 1994). Nor is it

sufficient for the opposing party simply to raise issues as to the credibility of the moving party's evidence. National Union Fire Ins. Co. v. Argonaut Ins. Co., 701 F.2d 95, 97 (9th Cir. 1983). If the nonmoving party fails to show that there is a genuine issue for trial, "the moving party is entitled to judgment as a matter of law." Celotex Corp., 477 U.S. at 323.

On motion for summary judgment, the court does not make credibility determinations, for "the weighing of evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge." Liberty Lobby, 477 U.S. at 249. Inferences to be drawn from the facts must be viewed in the light most favorable to the party opposing the motion. Masson v. New Yorker Magazine, 501 U.S. 496, 520 (1991).

DISCUSSION

Bernstein contends that the EAR's provisions still constitute prior restraint because they require him to apply for a license to engage in protected expression. Bernstein also argues that the EAR are content-based regulations of speech that violate the First Amendment by, among other requirements, compelling him to notify the government every time he changes encryption code while collaborating with a foreigner. Finally, Bernstein maintains that the EAR are vague and overbroad.

Defendants reply that Bernstein has not suffered the requisite injury in fact to support standing in this action, since the BIS has assured him in three advisory opinions that his activities are not subject to licensing by the EAR, and Bernstein has not submitted to BIS any of the encryption programs he contends could be subject to the EAR. Even if Bernstein does have standing, defendants argue that the EAR licensing provisions do not rise to the level of prior restraint. The notification provision, defendants contend, is a content-neutral regulation that satisfies intermediate scrutiny under the First Amendment.

I. The Current EAR

The Commerce Control List subjects certain types of "encryption software" to the EAR under Export Control Classification Number ("ECCN") 5D002. 15 C.F.R. § 774, Supp. 1. "Encryption software" is defined as "[c]omputer programs that provide capability of encryption functions or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software." Id. § 772.1. Encryption software that performs "authentication

or digital signature" functions, such as protecting PINs or passwords, is not regulated under ECCN 5D002. Id. § 774, Supp. 1, 5D002(c)(1), 5A002(a)(1).

The EAR prohibit export of any item subject to the EAR or re-export of any item of U.S. origin without a license. Id. § 736.2(b)(1). To be subject to the EAR, the item must first be in the United States or of U.S. origin. Id. § 734.3(a). Re-export and export from abroad of foreign-made encryption items such as software is also prohibited if there is any controlled U.S. content. Id. §§ 736.2(b)(2), 734.4(b). Thus, encryption software remains of U.S. origin even if it is "redrawn, used, consulted, or otherwise commingled abroad in any respect" with other software. Id. § 734.4(h). If "encryption software" is subject to the EAR because of "EI," or "Encryption Item," reasons,[3] then a license is required for export or re-export to every country except Canada. Id. § 742.15(a).

The EAR also prohibits export, re-export, or transfer of "any item subject to the EAR and exported or to be exported with knowledge" that a violation of the EAR "has occurred, is about to occur, or is intended to occur in connection with the item." 15 C.F.R. § 736.2(b)(10). "Knowledge" is defined to include "not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence." 15 C.F.R. § 772.1.

Export of encryption source code and object code is an "actual shipment, transfer, or transmission out of the United States" or a "transfer of such software in the United States to an embassy or affiliate of a foreign country." Id. § 734.2(b)(9)(I). Export includes downloading such code to "electronic bulletin boards, Internet file transfer protocol and World Wide Web sites" that can be accessed outside of the United States or "making such software available for transfer outside the United States" over such "communication facilities" as wire, cable or radio. Id. § 734.2(b)(9)(ii).

Re-export of software is defined as "an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country" or "release of . . . software subject to the EAR to a foreign national outside the United States." Id. 734.2(b)(4). Release is "visual inspection by foreign nationals of U.S.-origin equipment and facilities," "oral exchanges of information," or "application to situations abroad of personal knowledge or technical experience acquired in the United States." Id. § 734.2(b)(3). Any release to a foreign national is considered a re-export to the person's home country. Id. § 734.2(b)(5).[4]

Export and re-export of encryption source code and object code under ECCN 5D002 require a license unless there is an applicable exception. Id. § 736.2. Encryption source code and object code compiled from the source code may be exported or re-exported under the "technology and software unrestricted" ("TSU") license exception if the code is "publicly available." Id. § 740.13(e)(1), (e)(5). "Publicly available" code must "already [be] published or will be published," stem from "fundamental research," be "educational," or be part of certain patent applications. Id. § 734.3(b)(3). To be eligible for the exception, notification must be sent by email to the BIS "of the Internet location (e.g., URL or Internet address) of the source code or a copy of the source code *by the time of export*." Id. § 740.13(e)(5) (emphasis added). The TSU exception does not apply to knowing exports to terrorist countries, but posting code on the Internet does not establish such "knowledge." Id. § 740.13(e)(3), (4).[5]

"Technical assistance" concerning encryption software is an activity that is also subject to the EAR. Id. § 734.5. The EAR prohibit a "U.S. person" from providing "technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States of encryption commodities and software" that would fall under ECCN 5D002 if in the United States. Id. § 744.9(a). "Technical assistance" "[m]ay take forms such as instruction, skills training, working knowledge [and] consulting services." Id. § 772.1. The provision exempts assistance as to otherwise permissible exports, such as those subject to the TSU exception. Id. § 744.9(a). "[M]ere teaching or discussion of information about cryptography," such as "in an academic setting or in the work of groups or bodies engaged in standards development," does not establish the necessary intent "even where foreign persons are present." Id.

Violations of the EAR can result in administrative sanctions, civil penalties, or in the case of knowing violations, criminal penalties. Id. § 764.3. Willful violations by individuals can incur fines of up to $250,000 or ten years imprisonment. Id. § 764.3(b)(2)(I).

II. Standing

"[T]he irreducible constitutional minimum of standing" requires that there be injury in fact, a "causal connection" between the injury and the defendants' conduct, and a likelihood that the injury will be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992). The injury in fact must be both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."

Id. (quotations omitted). As the Ninth Circuit noted in Thomas v. Anchorage Equal Rights Commission, 220 F.3d 1134 (9th Cir. 2000), determining whether a plaintiff who brings a pre-enforcement challenge has shown injury in fact often implicates ripeness. Id. at 1139 ("We need not delve into the nuances of the distinction between the injury in fact prong of standing and the constitutional component of ripeness: in this case, the analysis is the same.").

Bernstein contends that he is injured because the following activities are prohibited without a license: (1) sharing encryption code with foreign persons at a conference in the United States, knowing that those persons do not comply with the EAR; (2) posting to the Internet encryption software written in assembly language; (3) posting to the Internet encryption software that has an "open cryptographic interface" which supports external software; (4) posting to the Internet an "Introduction to Cryptography" that explains how to write encryption source code; (5) posting to the Internet "mirrors" of encryption code found elsewhere; and (6) posting to an Internet newsgroup encryption source code, knowing that this code is sent to computers in Iran.[6] Bernstein also contends that he is injured because it is unclear whether encryption software intended to protect against forgery but that can also be used to protect against eavesdropping is subject to the EAR. Finally, Bernstein maintains that he is injured because it is impractical for him to take advantage of the TSU license exception when he is sharing encryption code with foreign persons at a conference in Canada.

To survive a motion for summary judgment, Bernstein must set forth facts showing that he faces "a realistic danger of sustaining a direct injury as a result of the statute's operation or enforcement." Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979). It is not enough to point to the "mere existence" of a statute to show injury; there must be a "'genuine threat of imminent prosecution.'" Thomas, 220 F.3d at 1139 (quoting San Diego County Gun Rights Comm. v. Reno, 98 F.3d 1121, 1126 (9th Cir. 1996). "In evaluating the genuineness of a claimed threat of prosecution," the Ninth Circuit looks to three factors: "whether the plaintiffs have articulated a concrete plan to violate the law in question; whether the prosecuting authorities have communicated a specific warning or threat to initiate proceedings; and the history of past prosecution or enforcement under the challenged statute." Id. (quotation omitted).

The first factor—a concrete plan— need not be "cast in stone," but it must be "something more than a hypothetical intent to violate the law." Id. at 1139. Bernstein has declared that the EAR keep him

from engaging in activities he would otherwise pursue. Thus, for example, Bernstein states that he is refraining from posting encryption code to the Internet because he does not know whether the code is subject to the EAR. Bernstein Dec. Supp. Pl.'s Mot. Summ. J. ¶¶ 135–59. Bernstein has also stated that he plans to refrain from collaborating with foreign colleagues at specific conferences in the United States and in Canada because he fears prosecution. Id. ¶¶ 23, 113, 119, 120–21 & 128.

These statements are sufficient to show a concrete plan. Unlike the plaintiffs in Thomas, who could not "specify when, to whom, where, or under what circumstances" they might violate the law, 220 F.3d at 1140, Bernstein has described particular situations where he claims he would violate the EAR if he did not censor his actions. Requiring Bernstein to state the day and time he planned to violate the law would turn this factor into a rigid formula. Taking all inferences in favor of Bernstein, as this court is required to do on a motion for summary judgment, Bernstein's statements clearly demonstrate "something more than a hypothetical intent to violate the law." Id. at 1139.

The second factor is a specific threat of enforcement toward Bernstein that is "credible," not "imaginary or speculative." Babbitt, 442 U.S. at 298. Bernstein need not wait until he is prosecuted before bringing a constitutional challenge, but he must show that he has "an actual and well-founded fear that the law will be enforced against him." Virginia v. American Booksellers Ass'n, 484 U.S. 383, 393 (1988). "When plaintiffs 'do not claim that they have ever been threatened with prosecution, that a prosecution is likely, or even that a prosecution is remotely possible,' they do not allege a dispute susceptible to resolution by a federal court." Babbitt, 442 U.S. at 298–99 (quoting Younger v. Harris, 401 U.S. 37, 42, 91 (1971)).

Bernstein has not set forth any facts showing a specific threat of enforcement. In response to Bernstein's inquiries, the BIS advised him in three opinions that he is no longer prohibited from exporting his encryption items and can now take advantage of the TSU license exception.[7] Bernstein maintains that BIS specifically threatened him in its advisory opinions when it stated that posting code to the Internet does not require a license "*provided that*" he supplied written notification of the web site or a copy of the source code. Kritzer Dec., Exh. 5, at 1–2 (emphasis in original). The emphasized words do not convert a description of the TSU license exception into a specific threat, particularly when Bernstein claims the

exception does not apply to his activities. At most, the statement makes clear that Bernstein must notify the BIS to take advantage of the TSU exception.

BIS specifically advised Bernstein that three of his activities do not need a license because they are subject to the TSU license exception. In its first opinion, BIS stated that Bernstein was not prohibited from assisting others with writing source code, even if the advice included actual source code, as long as the code was publicly available. Kritzer Dec., Exh. 3 at 3. The BIS later advised Bernstein that posting mirrors on the Internet is subject to the TSU license exception, and there is no duty to inquire whether the original document was posted in accordance with the EAR. Id., Exh. 5 at 2. When Bernstein asked if his "pre-export knowledge" that a newsgroup posting "fed into Iran as part of a general Usenet feed" was a violation of the regulations, Kritzer Dec., Exh. 2 at 2, the BIS responded that such knowledge would not "constitute a direct, knowing export," id., Exh. 4 at 3. Thus, there is clearly no threat of enforcement against Bernstein for posting "Introduction to Cryptography," mirroring documents or posting to newsgroups that are accessed in Iran.

Three more of Bernstein's activities concern specific types of encryption software that Bernstein claims, in strained readings of the EAR, either require a license or may require one. None of the advisory opinions indicate that Bernstein is prohibited from exporting these types of software.[8] Bernstein has not submitted any of the software to BIS for classification, as he did with the Snuffle program before he filed his first complaint.[9] Moreover, defendants have submitted a declaration by Bernard Kritzer, Director of the BIS office responsible for issuing advisory opinions, stating that the code his office found either on the Internet or in Bernstein's declarations was in fact subject to the TSU license exception. Kritzer Second Dec. ¶¶ 6–9. Kritzer also declared that the BIS did not treat assembly language code any differently than compiled code. Id. ¶ 10. Although such a declaration is not dispositive because it was prepared after the second supplemental complaint was filed, these statements taken together with a lack of any other evidence show no credible threat of enforcement against Bernstein for exporting these types of software.

The final two activities occur at conferences, where Bernstein shares encryption code with his colleagues. Bernstein contends that the BIS's decision not to enter into a stipulation waiving EAR requirements as to his conference activities is a specific threat of enforcement.[10] Contrary to Bernstein's characterization, the decision is not a threat to enforce the EAR against Bernstein for these activities, but a

refusal to exempt Bernstein from the reach of the EAR. Bernstein also finds a threat of enforcement in the following statement by BIS in its third advisory opinion: "[N]otification is required each time a new encryption algorithm in source code is made publicly available . . . . A new encryption algorithm is, with respect to a version previously notified, any algorithm that has been modified so that identical input results in different output."[11] Kritzer Dec., Exh. 5 at 2 n. 3. Such a general statement does not, however, rise to the level of a specific threat of enforcement for Bernstein's collaboration with foreign colleagues.

Bernstein maintains that a specific threat of enforcement exists because his activities could be prohibited by the EAR. Thus, for example, Bernstein claims he is chilled from posting assembly language code to the Internet because a literal reading of the EAR limits the TSU license exception to "compiled" source code. This argument finds some support in California Pro-Life Council, Inc. v. Getman, 328 F. 3d 1088 (9th Cir. 2003), where the Ninth Circuit held there was a specific threat of enforcement since the statute "appears to regulate" the planned activities. Id. at 1095 ("[F]ear of prosecution will only inure if the plaintiff's intended speech arguably falls within the statute's reach."). As California Pro-Life Council recognizes, however, the "self-censorship door to standing does not open for every plaintiff. The potential plaintiff must have 'an actual and well-founded fear that the law will be enforced against him.'" 328 F. 3d at 1095 (quoting Virginia v. American Booksellers Ass'n, 484 U.S. 383, 393 (1988)).

Bernstein has not put forth any facts to show his fear of enforcement is well-founded. His readings of the EAR, even if possible interpretations of the regulations' language, do not comport with the EAR's overall purpose or with any advice he has been given by the BIS. Simply because Bernstein can interpret the EAR to prohibit certain activities does not mean that those interpretations are reasonable. As the Ninth Circuit's most recent *en banc* decision on pre-enforcement challenges makes clear, "the mere existence of a proscriptive statute" is not enough to justify standing. Thomas, 220 F.3d at 1139.

The third factor is the history of enforcement under the EAR. Bernstein points to past enforcement against other cryptographers, a BIS Internet page that provides 2001 statistics about license applications, and a BIS press release about a company that settled allegations it exported encryption software without a license. Bernstein Dec. Opp. Defs.' Mot. Summ. J. ¶¶ 2–7. None of these examples are relevant to Bernstein's position. The past enforcement against cryptographers occurred under ITAR, not the EAR.[12] The statistics on the Internet do not prove anything more than that some exporters who applied for licenses

were denied them. Id., Exh. B at 94 ("the United States rejected five applications"). And the settlement in the press release was against a business that exported software to two firms in South Korea. Id., Exh. A. Where the record of enforcement is limited and of a different nature than the enforcement plaintiff fears, it does not show a history of enforcement adequate to support standing. Thomas, 220 F.3d at 1140–41.

Therefore, although Bernstein has demonstrated a concrete plan, he has not been subject to a specific threat of enforcement and cannot point to a history of enforcement that supports his claim of injury. As in Thomas, the threat of prosecution is "theoretically possible" but "not reasonable or imminent." Id. Even if Bernstein's injury were constitutionally sufficient for standing, prudential concerns of ripeness would counsel against accepting jurisdiction. "[T]o prevent courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements," courts must consider "the fitness of the issues for judicial decision" and "the hardship to the parties of withholding court consideration." Abbott Laboratories v. Gardner, 387 U.S. 136, 148, 149 (1967). Without a determination from BIS that a specific activity is prohibited by the EAR, there is no factual context for this court to resolve the constitutional challenges against the regulations. Moreover, defendants' repeated assurances that Bernstein is not prohibited from engaging in his activities weigh strongly against any hardship to Bernstein. If and when there is a concrete threat of enforcement against Bernstein for a specific activity, Bernstein may return for judicial resolution of that dispute.

Bernstein presented a concrete case or controversy when he first challenged the State Department's classification of his Snuffle computer program as a munition, and then again when control over the program was transferred to the Department of Commerce. Since then, the regulations governing export of encryption items have changed substantially. Bernstein no longer contends that he is prohibited from exporting Snuffle, but instead alleges a laundry list of activities that may or may not violate the EAR. In the process, this action has devolved into the world of hypotheticals, and like Thomas, is a "case in search of a controversy." Thomas, 220 F.3d at 1137.

CONCLUSION

For the foregoing reasons, Bernstein has failed to put forth specific facts demonstrating that he has standing to bring this action. The court therefore GRANTS defendants' motion for summary judgment and DENIES plaintiff's motion for summary judgment.

IT IS SO ORDERED.

Dated: July 28, 2003

_____/s/_____
MARILYN HALL PATEL
Chief Judge
United States District Court
Northern District of California

ENDNOTES

1. Because both defendants and plaintiff rely on materials outside the pleadings for their arguments—including whether plaintiff has standing—this court will treat defendants' motion as one for summary judgment. See Grove v. Mead School Dist. No. 354, 753 F.2d 1528, 1533 (9th Cir. 1985), cert. denied, 474 U.S. 826 (1985).

2. Facts are taken from this court's previous opinions or from the parties' submissions as noted.

3. Software is controlled for "EI" reasons under EAR if the software was an encryption item on the USML under ITAR. 15 C.F.R. § 774, Supp. 1.

4. Section 734.2(b)(9) specifically defines export of encryption software, but there is no similar provision defining re-export of such software. This leads to seemingly incongruous results. For example, release of encryption code to a foreign national in the United States is not an export under section 734.2(b)(9), while release to a foreign national in a foreign country would be a re-export under section 734.2(b)(4).

5. These countries are Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. 15 C.F.R. § 740.13(e)(4).

6. Bernstein argues in his motion papers that the EAR also prohibits him from publishing encryption software and technology because of its narrow definition of "published." Since Bernstein did not allege this activity in his complaint, the court will not address it.

7. Exporters may request an advisory opinion from the BIS on "whether a license is required, or likely to be granted, for a particular transaction," or "for guidance regarding other interpretations of the EAR." 15 C.F.R. § 748.3(a). Although BIS does not consider the opinions binding, id., the statements go to whether Bernstein's fear of prosecution was reasonable.

8. Even though the opinions did not specifically address these types of software, the context shows no threat of enforcement. Bernstein claims that he must get a license for export of programs written in assembly language, because the EAR defines "source code" as code that can be compiled, not assembled. When Bernstein asked BIS whether "interpretive languages [such as Perl and LISP] and other types of programs that do not fit into the regular source/object model" were considered source code or object code, Kritzer Dec., Exh. 1 at 9, BIS responded that "[e]ncryption programs written in programming languages such as PERL or LISP can be exported under license exception TSU if they meet" the publicly available requirement, id., Exh. 3 at 2. Although BIS did not specifically mention the assembly programming language, it is clear from this statement that the TSU exception covers more than code that is or can be "compiled." Similarly, in its discussion of open cryptographic interfaces, BIS does not give any indication that there is a separate category of such interfaces that would be prohibited because the interfaces are not considered "source code." Instead, the BIS states in its advisory opinion that source code is subject to TSU exception even if includes an open cryptographic interface. Id., Exh. 3 at 2.

9. When Snuffle became subject to the EAR, BIS admitted that the regulatory framework as applied to the program remained the same; therefore, it was not necessary for Bernstein to request another classification to have standing.

10. The proposed stipulation read: "The Secretary [of Commerce] will not impose, or seek or encourage the imposition of, civil penalties or criminal sanctions for the 2002 Conference Activities. If the Export Administration Regulations...impose any licensing requirements, notification requirements, or other requirements upon the 2002 Conference Activities, the Secretary hereby waives those requirements as applied to the 2002 Conference Activities." Bernstein Dec. Opp. Defs.' Mot. Summ. J. ¶ 9. Defendants' attorney stated that defendants "obviously cannot stipulate, as you propose, that Dr. Bernstein or any other individual is exempt from the EAR." Id., Exh. D at 1. Bernstein informed defendants that he understood this decision "as a specific threat of punishment under EAR for some or all of the 2002 Conference Activities." Id., Exh. E at 2.

11. At oral argument, Bernstein contended that the purpose of collaborating with his colleagues is to change the algorithm such that it results in a different output. Each "tweaking" of the code thus results in a new algorithm, requiring notification.

12. Another cryptographer, for example, posted encryption software on the web and then received a letter from the Department of State warning that the software needed a license under ITAR. Demberger Dec. ¶¶ 2–3.